Cyber risks your business could face during a pandemic

Submitted by **Reza Kamrani, Account Representative, Associations** | www.federated.ca

During a pandemic, there are a number of things business owners need to think about, ranging from the safety of their employees to their bottom line. But one area of risk, that you may overlook, is cybercrime.

Opportunistic hackers may see a pandemic as a chance to attack while organizations are distracted and dealing with the challenges a situation like that can bring with it. That's why it's vital to know what the risks are, and what you and your employees can do to combat cybercrime.

Social engineering

The vast majority of cyber-attacks – by some estimates, 98 per cent – deploy social engineering methods. They exploit fear and uncertainty to trick users and gain access to their passwords, networks, and data. Recently, cyber criminals have been using the fear surrounding the COVID-19 pandemic to their advantage.

One method they've used to do this is through phishing e-mails. Phishing is a type of cybercrime during which fraudulent communications are used to trick users into revealing things like passwords or credit card information. The communications can also be used to gain access to a business' network. Phishing can occur in a variety of mediums, ranging from emails to phone calls to text messages or even faxes.

This form of cybercrime is by no means new. Historically, scammers have utilized a number of tactics, including posing as members of the Canadian Revenue Agency or as law enforcement officers to trick people into revealing personal information.

With COVID-19 cases on the rise, phishing e-mails have begun popping up in which scammers pose as health professionals, claiming to represent well-known organizations like The Canadian Red Cross or World Health Organization. They do this with the intention of tricking people into downloading malware or clicking malicious links. Because of this, even if an email claims to have information about the pandemic, be sure to read it carefully to make sure it's legitimate.

A recent malware attack took advantage of internet users' interest in information about the coronavirus. The malware attack aimed at those looking for cartographic presentations of the spread of COVID-19 online and tricked them into downloading and running a malicious application which compromised their computer. To help combat situations like this, employee's computers should have adequate firewalls in place, and they should be instructed to stay away from websites not pertaining to their work while on their work computer.

Vulnerabilities at home

During a pandemic, health concerns can lead some companies to have employees begin working from home. While this is great from a public health standpoint, it can open businesses up to a variety of cyber exposures they wouldn't otherwise have to worry about. With everyone relying on digital infrastructure more than ever, the cost of an attack could be very high.

With employees working from home, companies should ensure they have a Virtual Private Network (VPN) in place. It allows employees a secure way to access their work network from home. Multi-factor authentication should also be utilized for accessing email and virtual networks. Lastly, employees should be reminded to have long, complex passwords for their home Wi-Fi networks and to never re-use passwords across the Internet.

Microsoft offers various services that could help your employees work efficiently while at home. These include training materials for Microsoft Teams, Office 365, and Windows 10. To learn more, visit their health and training website.

Employee error

Employees who are working in unfamiliar places and distracted by the pandemic – and the effects it could have socially, economically, and financially – may be more likely to make mistakes they wouldn't otherwise. This can open companies up to hackers who use various techniques (like phishing) to trick employees. To combat this, education is key. Confirm that your employees are aware of the various types of cybercrime and how to spot them. Also, be sure to educate them on the technology involved when working from home (e.g. how to log onto the VPN). This will ensure employees are less likely to panic and make mistakes.

Ensure you're protected

Making sure your company's cyber security efforts are up-to-date and that your employees are aware of the risks and how to mitigate them is key. But on top of that, it's important to ensure you have the necessary coverage should something go wrong. Cyber risk coverage is designed to support your business if computer networks are breached. Reach out to your broker to find out if you're adequately protected or visit our cyber risk coverage page to find out more!

Reza Kamrani is the Account Representative for Associations at Federated Insurance.